UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/582,803	06/14/2006	Yuichi Futa	2006_0892A	4687

52349   7590   05/27/2009
WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER
NGUYEN, MINH DIEU T

ART UNIT	PAPER NUMBER
2438	

MAIL DATE	DELIVERY MODE
05/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
	10/582,803	FUTA ET AL.
Office Action Summary	Examiner	Art Unit	
	MINH DIEU NGUYEN	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _05 March 2009_.
2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-15,18-21 and 24_ is/are pending in the application.
    4a) Of the above claim(s) _16,17,22 and 23_ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-9,18-21 and 24_ is/are rejected.
7)☒ Claim(s) _10-15_ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☐ All   b)☐ Some * c)☐ None of:
      1.☐ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This office action is in response to the communication dated 3/5/2009.

2.   Claims 1-15, 18-21 and 24 are pending. Claims 16-17 and 22-23 are being

cancelled.

Response to Arguments

3.   Applicant's arguments filed 3/5/2009 have been fully considered but they are not

persuasive. The Applicant argues that Peyravian does not disclose generating random

information R based on the read unique management information and using the read

prime q and the generated random information R to calculate N according to N= 2 x

random information R x prime q +1. The Examiner respectfully disagrees, AAPA

discloses the Pocklington's primality test is used to test primality of calculated prime

candidate N according to N = 2 x random number R x prime q + 1 (AAPA: 0030). AAPA

does not explicitly teach random number R is generated based on the unique

management information. Peyravian discloses his algorithm will guarantee that all of the

primes generated by different users are different and are ultimately tied up to user-

specific data (Peyravian: Section 2, the 12th paragraph on page 284) and the users'

unique characteristics can be a user identifier, device identifier, or company identifier

(Peyravian: Section 8 on page 287). As such to make the information random and user-

specific so the prime numbers and RSA keys can be checked for repudiation, it is

obvious to combine the teaching of AAPA and Peyravian.

Claim Objections

4.   Claim 10, 14, 18 and 20-21 are objected to because of the following informalities:

a)   As to claim 10, the phrase "multiplying the management information" should be – multiplying the **unique** management information --.

b)   As to claim 21, the phrase "and a secondary information storage unit storing a predetermined verification calue" should be -- and a secondary information storage unit storing a predetermined verification **value**--.

c)   As to claim 24, the phrase "the primality testing unit is operable totest primality of the calculated prime candidate N" should be -- the primality testing unit is operable **to test** primality of the calculated prime candidate N--.

The limitation of claim 24 depends on claim 1, however that exact limitation is already recited in claim 1. As such, the same limitation is duplicated.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

5.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6.   Claim 20 is rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claim recites a series of steps or acts to be performed, a statutory "process' under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. See page 10 of In Re Bilski 88 USPQ2nd 1385. The instant

claim is neither positively tied to a particular machine that accomplishes the claimed

method steps nor transform underlying subject matter, and therefore does not qualify as

a statutory process.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 1-9, 18, 20-21 and 24 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Applicant Admitted Prior Art (AAPA) in view of Peyravian et al.

("Generation of RSA Keys That Are Guaranteed to be Unique for Each User).

        a)   As to claims 1, 20-21 and 24, AAPA discloses a prime calculating

apparatus for calculating a prime candidate N larger than a known prime q and testing

primality of the calculated prime candidate N, comprising:

        a prime storage unit storing the known prime q; a random information generation

unit operable to generate random information; a candidate calculation unit operable to

read the prime q from the prime storage unit, and calculate the prime candidate N using

the read prime q and the generated random information R, according to N= 2 x random

information R x prime q + 1; a primality testing unit operable to test primality of the

calculated prime candidate N according to the Pocklington's primality test (AAPA:

0030); and an output unit operable to output the calculated prime candidate N as a

prime N when the primality of the calculated prime candidate N is determined (AAPA:

0024-0030). AAPA is silent on the capability of having unique management information

and generating random information R based on the unique management information.

Peyravian is relied on for the teaching of having unique management information and

generating random information R based on the unique management information

(Peyravian: sections 2-4). It would have been obvious to one of ordinary skill in the art

at the time of the invention to employ the use of having unique management information

and generating random information R based on the unique management information in

the system of AAPA, as Peyravian teaches, so as to offer much stronger uniqueness

and protection to system.

     b)   As to claims 2-3, the combination of AAPA and Peyravian discloses the

random information generation unit includes: a reading subunit operable to read the

unique management information from the management information storage unit; a

random number calculation unit operable to calculate a random number r; a combining

subunit operable to make a combination of the read unique management information

and the generated random number r; and a computation subunit operable to compute

the random information R based on the combination by applying an injection function to

the combination (Peyravian: section 3).

     c)   As to claim 4, exclusive-or function is a well-known, standard operation on

bits. It can be used to XOR a plaintext with a keyword to generate a ciphertext. It is a

designed choice to apply XOR function to the key information and the combination as

claimed.

d)   As to claim 5, the combination of AAPA and Peyravian discloses

calculating the prime candidate N having a bit length twice a bit length of the prime q,

wherein the random number calculation subunit calculates the random number r, a bit

size of which is obtained by subtracting a bit length of the unique management

information and 1 from the bit length of the prime q (i.e. random number r having length

(q) -1 bit, random information R is a combination of random number r and management

information as disclosed by Peyravian, therefore the bitsize of random number r is

obtained by subtracting a bit length of the unique management information and 1 from

the bit length of the prime q, AAPA: 0024).

e)   As to claim 6, the combination of AAPA and Peyravian discloses the

primality testing unit includes: a first judging subunit operable to judge whether the

prime candidate N satisfies $2^{N-1} = 1 \mod N$; and a second judging subunit operable to

perform, when the judgment of whether the prime candidate N and the random

information R satisfy $2^{2R} \neq 1 \mod N$, and to determine the primality of the prime

candidate N when the performed judgment is affirmative (AAPA: 0030, 0032-0033).

f)   As to claim 7, the combination of AAPA and Peyravian discloses the

primality testing unit includes: a first judging subunit operable to judge whether the

prime candidate N satisfies $2^{N-1} = 1 \mod N$; and a second judging subunit operable to

perform, when the judgment of whether the prime candidate N and the random

information R satisfy GCD(2^{2R} -1, N) =1, and to determine the primality of prime

candidate N when the performed judgment is affirmative (AAPA: 0027, 0028).

g)   As to claims 8-9, the combination of AAPA and Peyravian discloses an

iteration control unit operable to control the random information generation unit, the

candidate calculation unit, and the primality testing unit to iterate the generation of the

random information R, the calculation of the prime candidate N, and the primality testing

until the primality of the calculated prime candidate N is determined by the primality

testing unit (AAPA: 0029), the iteration control unit therefore iterates the random

information R', calculates N'=2 x random information R' x prime N +1 and tests the

primality of N' and continues with the iteration steps.

h)   As to claim 18, the majority of this claim is addressed in claims 1 and 8,

with the addition of a key issuing server apparatus for generating and issuing the private

key and the public key of RSA encryption for a terminal further comprising a key output

unit operable to output the generated private key to the terminal; and a publishing unit

operable to publish the generated public key that is addressed by the combination of

AAPA and Peyravian discloses (AAPA: 0004).

9.   Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over

Applicant Admitted Prior Art (AAPA) in view of Peyravian et al. ("Generation of RSA

Keys That Are Guaranteed to be Unique for Each User) and further in view of Oka et al.

(2002/0108042).

The combination of AAPA and Peyravian is silent on the capability of having a certificate issuing server apparatus, wherein the key output unit outputs the public key to the certificate issuing server apparatus and the certificate issuing server apparatus includes: a storage unit storing a private key of the certificate issuing server apparatus; an obtaining unit operable to obtain the public key; a certificate generation unit operable to (i) generate signature data by applying a digital signature to public key information including the public key, using the private key of the certificate issuing server apparatus, and (ii) generate a public key certificate including at least the public key and the generated signature data; and an output unit operable to output the generated public key certificate to the key issuing server apparatus. Oka is relied on for the teaching of having a certificate issuing server apparatus, wherein the key output unit outputs the public key to the certificate issuing server apparatus and the certificate issuing server apparatus includes: a storage unit storing a private key of the certificate issuing server apparatus; an obtaining unit operable to obtain the public key; a certificate generation unit operable to (i) generate signature data by applying a digital signature to public key information including the public key, using the private key of the certificate issuing server apparatus, and (ii) generate a public key certificate including at least the public key and the generated signature data; and an output unit operable to output the generated public key certificate to the key issuing server apparatus (Oka: 0001, 0018-0019, Fig. 2-3, 8). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having a certificate issuing server apparatus, wherein the key output unit outputs the public key to the certificate issuing server

apparatus and the certificate issuing server apparatus includes: a storage unit storing a

private key of the certificate issuing server apparatus; an obtaining unit operable to

obtain the public key; a certificate generation unit operable to (i) generate signature data

by applying a digital signature to public key information including the public key, using

the private key of the certificate issuing server apparatus, and (ii) generate a public key

certificate including at least the public key and the generated signature data; and an

output unit operable to output the generated public key certificate to the key issuing

server apparatus in the system of AAPA and Peyravian, as Oka teaches, so as to

provide public key certificate for users.

Allowable Subject Matter

10.   Claim 10 would be allowable if rewritten to overcome the claim objection set forth

in this office action. Claims 11-15 depends on claim 10 and would be allowable.

Conclusion

11.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

         A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the date of this final action.

12.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-

3873.

        If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Taghi T. Arani can be reached on 571-272-3787. The fax phone number for

the organization where this application or proceeding is assigned is (571) 273-8300.

        Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status

information for unpublished applications is available through Private PAIR only. For

more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business

Center (EBC) at 866-217-9197 (toll-free).

/Minh Dieu Nguyen/
Primary Examiner, Art Unit 2438